Hochschule Hannover

University of Applied Sciences and Arts

Fakultät I – Elektro und Informationstechnik

Fachgebiet: Automatisierungstechnik und Prozessinformatik

– Leitfaden –

„Einführung eines Informationssicherheitsmanagementsystems bei kleinen und mittleren Unternehmen“

Autor: Marian Thöne

Erarbeitet im Rahmen einer Bachelorarbeit.

Erstprüfer: Prof. Dr.-Ing. Karl-Heinz Niemann

Zweitprüfer: M. Eng. Jan-Niklas Puls

I Versionshistorie und Lizenzinformationen

Version	Datum	Bemerkung	Erstellende Person
1.0	02.07.2023	Erstausgabe	MarTh
1.1	31.07.2023	Korrigierte Erstausgabe – Kommentare von Erst- und Zweitprüfer – Hinzufügen der „CC BY 4.0“ Lizenz	MarTh
1.2	22.09.2023	Einarbeitung von weiteren Korrekturen	Jan-Niklas Puls
2.0	12.10.2023	Zweitausgabe (Veröffentlichung) – Einpflegen von Kommentaren – Hinzufügen des Haftungsausschlusses – Hinzufügen des Autors	MarTh
2.1	23.10.2023	Hinzufügen der DOI	MarTh

Der Leitfaden wurde als Teil einer Bachelorarbeit während der Kooperation der Hochschule Hannover mit dem Mittelstand-Digitalzentrum Hannover erarbeitet.

https://doi.org/10.25968/opus-2980

II Haftungsausschluss

Die diesem Dokument zu Grunde liegenden Informationen wurden mit größtmöglicher Sorgfalt recherchiert und zusammengestellt. Dennoch wird es ohne eine Gewährleistung zur Verfügung gestellt. Der Autor lehnt ausdrücklich jede Art von vertraglicher oder gesetzlicher Haftung für dieses Dokument ab. In keinem Fall ist der Autor für Schäden verantwortlich, die durch Fehler oder fehlende Informationen in diesem Dokument entstehen könnten. Logos und Markennamen werden ohne Hinweis auf ggf. bestehende Schutzrechte verwendet.

III Inhaltsverzeichnis

I Versionshistorie und Lizenzinformationen II
II Haftungsausschluss III
III Inhaltsverzeichnis IV

1 Warum dieser Leitfaden? 1
2 Leitfaden zur Einführung eines ISMS bei KMU – Aufbau 4
3 Leitfaden zur Einführung eines ISMS bei KMU – Erläuterungen 5
4 Leitfaden zur Einführung eines ISMS bei KMU – Schritte 6
Schritt 1: Analyse des Unternehmens 6
Schritt 2: Informationssicherheitsleitlinie 10
Schritt 3: Risikoanalyse 11
Schritt 4: Organisation der IT-Sicherheit 14
Schritt 5: Informationssicherheitsrichtlinien (ISR) 16
5 Leitfaden zur Einführung eines ISMS bei KMU – Abschluss 40
6 Abbildungsverzeichnis 41
7 Abkürzungsverzeichnis/Glossar 42
8 Literatur 45

1 Warum dieser Leitfaden?

Die Sicherheit von Informationen gewinnt für Unternehmen in den letzten Jahren an immer größerer Bedeutung, nicht nur durch das stetig steigende, sondern auch durch die ökonomische Bedeutung von Sicherheitsvorfällen.

Das belegt auch eine kürzlich veröffentlichte Studie (TÜV Cybersecuritystudie 2023), die vom TÜV-Verband in Auftrag gegeben wurde [1–3].

- 98 % der befragten Unternehmen empfinden Cyberangriffe als ernste Gefahr.
- 76 % der befragten Unternehmen sehen Vorteile in einem hohen IT-Sicherheitsniveau.

Die Bedeutung der Informationssicherheit bei Unternehmen in Deutschland weist laut dieser Studie große Unterschiede je nach Größe des Unternehmens auf.

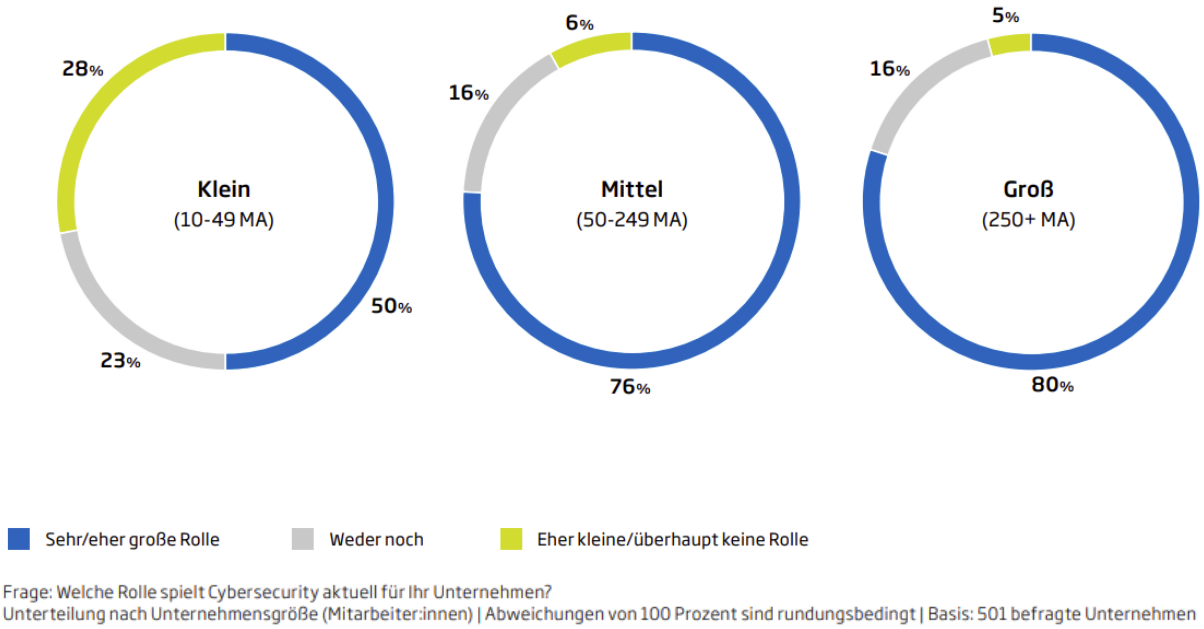

Abbildung 1: Bedeutung der Cybersecurity in Unternehmen [1, S. 8]

Abbildung 1 zeigt, dass bei größeren Unternehmen mit mehr als 250 Mitarbeitenden lediglich bei etwa 5 % der Unternehmen die Informationssicherheit nahezu keine Rolle spielt. Je kleiner die Unternehmen werden, desto größer wird der Anteil der Unternehmen, bei denen die Informationssicherheit keine größere Rolle spielt. In dieser Erhebung wurden lediglich Unternehmen mit mehr als zehn Mitarbeitenden befragt. Die Tendenz der Grafik lässt aber darauf schließen, dass die Rolle der Informationssicherheit bei Unternehmen mit weniger als zehn Mitarbeitenden noch geringer ausfallen wird, als bei kleinen und mittleren Unternehmen [3, S. 8].

Um diese Tendenz aufzuhalten, bietet ein Informationssicherheitsmanagementsystem (ISMS), basierend auf (inter-)nationalen Normen, eine Grundstruktur für den effizienten und effektiven Umgang mit einer ganzheitlichen Sicherheitsstrategie. [4, S. 5]

Eine solche ganzheitliche Sicherheitsstrategie ist sowohl für produzierende als auch nicht produzierende Unternehmen von Bedeutung.

In der Wissenschaftsdokumentation „Cybercrime – Wie können wir uns schützen?“ ergab ein Test, dass viele Steuerungen von Produktionsmaschinen noch immer frei über das Internet zugänglich sind und von Dritten kontrolliert werden können. Von der Manipulation des Lichtes bis zur Steuerung von kritischen Ventilen oder ganzen Maschinen gäbe es zahlreiche Angriffsmöglichkeiten. Dieses Beispiel zeige sehr deutlich den Handlungsbedarf bei produzierenden Unternehmen – insbesondere bei sehr kleinen, kleinen und mittleren Unternehmen [5].

Abhängig von der Branche und den zu schützenden Informationen variiert die Ausrichtung der Ziele des ISMS. Die Erreichung dieser Ziele insbesondere bei KMU erfordert aufgrund von fehlender Praxis und fehlenden Ressourcen ein gewisses Maß an Anpassung und näheren Erläuterungen.

Der vorliegende Leitfaden zur Einführung eines ISMS bei KMU basiert im Wesentlichen auf den VdS-Richtlinien VdS 10000 [6] und VdS 10005 [7]. Er enthält eine grundlegende Zusammenstellung der Forderungen aus den zurzeit relevanten (inter-) nationalen Vorschriften und Normen und richtet sich an die Unternehmen, die ein ISMS zur Sicherheit Ihres Unternehmens aufbauen oder optimieren wollen.

Für größere KMU sind auch die Normen der DIN EN ISO/IEC 27000-Normenfamilie relevant. Der Fokus liegt in diesem Leitfaden jedoch auf den kleineren KMU.

Bei kleinen Unternehmen ist der Anteil derer, die ihre Informationssicherheit nicht auf der Basis von Normen und Standards implementieren, mit 38 % sehr hoch – bei mittleren Unternehmen ist dieser mit 12 % deutlich geringer. Mithilfe dieses Leitfadens sollen auch kleine Unternehmen unterstützt werden, ihre Informationssicherheit durch Normen und Standards zu verbessern [3, S. 42].

Der Leitfaden ist ein eigenständiges und in sich abgeschlossenes Dokument. Es versetzt den Anwendenden in die Lage, mit einer Art Checkliste das ISMS ohne Vorkenntnisse zu etablieren. Durch die Beschreibung von Zielen und weitergehenden Erläuterungen werden die Anwendenden zielgerichtet zu einem ISMS geführt. Als „Schritt-für-Schritt-Bedienungsanleitung“ bzw. Schilderung der genauen Umsetzung ist dieser Leitfaden jedoch nicht anzusehen, da dies nicht das Ziel eines Leitfadens darstellt. Ein Leitfaden soll leiten, aber nicht die genaue Vorgehensweise vorgeben. Deswegen werden in vielen Fällen nur Beispiele und Hilfen angeführt und es wird auf die relevanten Normen und Richtlinien verwiesen, sodass das Grundkonzept umgesetzt werden kann.

Sofern weitere Informationen erforderlich sind, wird in jedem Schritt des Leitfadens auf die entsprechenden Normen verwiesen, sodass dort die weiterführenden Informationen entnommen werden können. Für Unternehmen bis 50 Mitarbeitende ist darüber hinaus ein Blick in die seit 2023 veröffentlichte und frei zur Verfügung stehende DIN SPEC 27076 empfehlenswert. Hier werden Problemstellungen und potentielle Lösungsmaßnahmen vorgestellt.

Allgemein wird zwischen produzierenden und nicht produzierenden Unternehmen unterschieden. Der Leitfaden gilt hierbei generell für alle Unternehmen. Bei produzierenden Unternehmen sind einige Maßnahmen jedoch nicht umsetzbar. Einige dieser Ausnahmen sind im Leitfaden angemerkt. Die Umsetzung dieser Maßnahmen ist jedoch nicht Bestandteil des Leitfadens. Für die besonderen Anforderungen von industriellen Automatisierungssystemen können interessierte Unternehmen die Maßnahmen und technischen Aspekte in der Norm DIN EN IEC 62443-2-1 [8] und der Richtlinie VdS 10020 nachlesen.

Zu Beginn wird in Kapitel 2 der Aufbau des Leitfadens mithilfe eines Schaubildes visualisiert. Im darauffolgenden Kapitel (Kapitel 3) werden dann die einzelnen Schritte des Schaubildes aus Kapitel 2 erklärt, bevor diese in Kapitel 4 detailliert beschrieben werden. Kapitel 5 schließt den Leitfaden ab.

*Laut der TÜV Cybersecurity Studie 2023 sagen **lediglich etwa 18 %** der Befragten, dass die Informationssicherheit die **Produktivität des Unternehmens verringere** bzw. neue **Innovationen hemmt*** [3, S. 23].

An diesem Zitat wird deutlich, dass die Mehrheit der Befragten keine oder nur sehr geringe Beeinträchtigungen durch die Implementierung eines ISMS erwartet.

2 Leitfaden zur Einführung eines ISMS bei KMU – Aufbau

Das nachfolgende Schaubild zeigt den Aufbau des Leitfadens. Diese Farben finden sich ebenfalls in den Rahmen der einzelnen Schritte der detaillierten Beschreibungen in Kapitel 4 wieder.

3 Leitfaden zur Einführung eines ISMS bei KMU – Erläuterungen

Dieses Kapitel dient als Information, um den Aufbau des nächsten Kapitels zu erklären und den Umgang damit zu erleichtern.

Jeder Schritt im nächsten Kapitel besteht immer aus den folgenden Bereichen:

Schritt: Titel

Verantwortlichkeiten:

- Hier werden die Verantwortlichkeiten des Vorgangs definiert und ggf. Aufgaben dieser in Bezug auf den Vorgang beschrieben.

Ziele:

- Hier werden die Ziele dargestellt.
- Was wird verfolgt bzw. soll erreicht werden?

Aktivität:

- Nach der Formulierung der Ziele, werden in diesem Bereich die Aktivitäten zur Erreichung der Ziele aufgeführt.

Erläuterung der Aktivitäten:

- Sind die Aktivitäten nicht eindeutig, folgen in diesem Abschnitt Erklärungen und Hilfestellungen. Diese sind jedoch nur als Hilfestellungen zu betrachten.
- Oftmals wird in den Erläuterungen auf ein externes Dokument verwiesen, da die genaue Umsetzung in diesem Leitfaden zu umfangreich wäre.
- Teilweise werden hier auch Ergebnisse der TÜV Cybersecurity Studie 2023 [3] zur Verdeutlichung des Stellenwertes angegeben.

Manche Schritte und Informationssicherheitsrichtlinien sind in den VdS-Richtlinien für sehr kleine und/oder kleine Unternehmen nicht vorgesehen. Die Kennzeichnung dazu erfolgt mittels Fußnoten.

Wie im vorherigen Kapitel schon erwähnt, deutet die Farbe des Rahmens auf den jeweiligen Schritt im Schaubild des Leitfadens hin.

4 Leitfaden zur Einführung eines ISMS bei KMU – Schritte

Schritt 1: Analyse des Unternehmens

Verantwortlichkeiten:

- Die Geschäftsleitung gibt die Analyse des Ist-Zustandes des Unternehmens in Auftrag oder führt diese selber aus und ist für das Ergebnis verantwortlich.

Ziele:

- Übersicht aller vertraglichen Anforderungen und gesetzlichen Vorschriften
- Übersicht aller Stakeholder und Stakeholderinnen
- Scope-Dokument (Dokument über den Geltungsbereich)
- Erklärung zur Anwendbarkeit (SoA)

Aktivität:

- Analyse der Verträge des Unternehmens hinsichtlich der Anforderungen in Bezug auf die Informationssicherheit.
- Analyse der gesetzlichen Vorschriften, die das Unternehmen und Ihre Branche betreffen, in Bezug auf die Informationssicherheit.
- Ausführliche Bestimmung der **Stakeholder und Stakeholderinnen** und die Bedeutung jedes/jeder Einzelnen.
- Bestimmung des **Geltungsbereich** des ISMS und Durchführung einer Umfeldanalyse (relevante organisatorische und technische Schnittstellen).
- Analyse der Anwendbarkeit der Maßnahmen zur Informationssicherheit in dem Unternehmen und Dokumentation des Ergebnisses in der sogenannten „**Erklärung zur Anwendbarkeit**“ (SoA – engl. **S**tatement **o**f **A**pplicability).

Erläuterung der Aktivitäten:

- Analyse der Verträge des Unternehmens hinsichtlich der Anforderungen in Bezug auf die Informationssicherheit.
  - Welche Daten gibt es im Unternehmen und wo werden diese gelagert?
  - Welche Hard-/Software wird verwendet?
  - Wer ist im Unternehmen für die Informationssicherheit zuständig?
  - Wer trägt die Gesamtverantwortung für die Informationssicherheit im Unternehmen?
  - Weitere beispielhafte Fragen können in dem kostenfrei zur Verfügung stehenden Dokument „**DIN SPEC 27076**“ [8] nachgelesen werden.
- Analyse der gesetzlichen Vorschriften, die das Unternehmen und die Branche betreffen, in Bezug auf die Informationssicherheit.
  - IT-SiG 2.0 – IT-Sicherheitsgesetz 2.0
  - NIS-Richtlinie – Richtlinie für die Gewährleistung einer hohen Netzwerk- und Informationssicherheit (nur für KRITIS relevant)
  - NIS-2-Richtlinie – Nachfolger der NIS-Richtlinie

    (wird aktuell in nationales Recht überführt)
  - TTDSG – Telekommunikation-Telemedien-Datenschutz-Gesetz
  - DSGVO – Datenschutzgrundverordnung
  - Aktien- und GmbH-Recht – Vorgaben zum Risikomanagement
  - KRITIS 2.0 – Verordnung zur Bestimmung von kritischen Infrastrukturen
    Info: Dieser Leitfaden bezieht sich **nicht** auf KRITIS-Unternehmen. Der Vollständigkeit halber ist die Verordnung hier trotzdem aufgeführt
  - EU Cyber Resilience Act [9]
  - weitere Gesetze und Vorschriften z. B. von der Handwerkskammer
- Ausführliche Bestimmung der **Stakeholder und Stakeholderinnen** und die Bedeutung jedes/jeder Einzelnen.
  - Kunden/Kundinnen, Lieferanten/Lieferantinnen, Dienstleistende, Gesetzgeber/Gesetzgeberinnen, Gläubiger/Gläubigerinnen, Gesellschaft
  - Mitarbeitende, Manager/Managerinnen, Eigentümer/Eigentümerinnen

- Bestimmung des **Geltungsbereichs** des ISMS und Durchführung einer Umfeldanalyse (relevante organisatorische und technische Schnittstellen).

  Info: Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in der VdS Richtlinie VdS 10005 nicht vorgeschrieben.

  - Erstellung eines Netzstrukturplan aller maßgeblichen Systeme und Komponenten
  - Das BSI bietet hierzu eine Informationsseite auf seiner Homepage an, auf welcher die Wahl des Geltungsbereiches beschrieben wird [10].
  - ISO 31000:2018 – 6.3.2 und 6.3.3 stellen Leitfäden für die Vollständigkeit der Dokumentation zur Verfügung [11]

  Analyse der Anwendbarkeit der Maßnahmen zur Informationssicherheit in dem Unternehmen und Dokumentation des Ergebnisses in der

  „**Erklärung zur Anwendbarkeit**“ (SoA).

  Info: Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in der VdS-Richtlinie VdS 10005 nicht vorgeschrieben.

  In einer solchen Erklärung zur Anwendbarkeit steht die Anwendbarkeit der Maßnahmen aus dem Anhang A der ISO 27001 [12]. Diese Erklärung kann mittels einer Tabelle durchgeführt und dokumentiert werden.
  Eine mögliche Tabellenstruktur wird nachfolgend dargestellt.

Tabelle 1: Beispielhafte Tabellenstruktur zur Umsetzung einer SoA

Maßnahmen	Anforderungen			Umsetzung	Status
	Vertraglich	Gesetzlich	Regulatorisch		
Überprüfung der Informationssicherheitsrichtlinien					
Informationssicherheitsrollen und -verantwortlichkeiten					
Sicherheitsüberprüfung					
…					

Diese Tabelle stellt lediglich eine beispielhafte Struktur dar und ist individuell auf die jeweiligen Bedürfnisse anzupassen. Zudem sollte diese Tabelle um die im Anhang A der DIN EN ISO/IEC 27001 [12] stehenden Anforderungen ergänzt werden.
Für eine Zertifizierung ist es Pflicht, diese Anforderungen zu berücksichtigen.

Schritt 2: Informationssicherheitsleitlinie [1]

Verantwortlichkeiten:

- Die Geschäftsleitung ist für die Inkraftsetzung einer Informationssicherheitsleitlinie verantwortlich und muss dafür sorgen, dass diese jährlich geprüft und ggf. aktualisiert wird.

Ziele:

- Mit dieser Leitlinie soll der Stellenwert der Informationssicherheit im Unternehmen festgelegt werden.

Aktivität:

- Erstellung einer Informationssicherheitsleitlinie.

Erläuterung der Aktivitäten:

Erstellung einer Informationssicherheitsleitlinie.

- Festlegung der Ziele und des Stellenwertes der Informationssicherheit im Unternehmen
- Definition aller erforderlichen Positionen und deren Aufgaben im Unternehmen
  - Geschäftsleitung
  - Informationssicherheitsbeauftragter/Informationssicherheitsbeauftragte
  - Informationsverantwortlicher/Informationsverantwortliche
  - Systemadministrator/Systemadministratorin
  - Projektverantwortliche
  - Externe (Lieferanten/Lieferantinnen)
  - Datenschutzbeauftragte(r)
  - Betriebsrat (Mitarbeitende)
  - Vorgesetzte
- Angaben von Konsequenzen bei Nichtbeachtung der Leitlinie.
- Das BSI hat für ein fiktives Unternehmen eine komplette Analyse durchgeführt und u. a. auch eine Sicherheitsleitlinie erstellt. Diese kann im Verweis [13] im Literaturverzeichnis nachgelesen werden und als Arbeitsgrundlage dienen.

[1] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Schritt 3: Risikoanalyse [2]

Verantwortlichkeiten:

- Die Geschäftsleitung ist für die verantwortungsbewusste Durchführung verantwortlich.

Ziele:

- Ausführliche Risikoanalyse der Informationssicherheit des Unternehmens

Aktivität:

- Durchführung einer ausführlichen Risikoanalyse.

Erläuterung der Aktivitäten:

- Eine Risikoanalyse besteht aus der **Identifikation**, der **Analyse** und der **Bewertung** von Risiken und definiert den IST-Zustand des Unternehmens.
- Nach dem BSI 200-3 Standard [14] sind folgende vier Schritte A – D für eine Risikoanalyse vorgesehen:

  A) Erstellung einer Gefährdungsübersicht (elementare und spezifische Gefährdungen) – (Kapitel 4 des BSI 200-3)

  - elementare Gefährdung: Feuer, Wasser, Naturkatastrophen, Stromausfall
    Info: Bei produzierendem Gewerbe ist dies ein wichtiger Punkt in der Risikoanalyse, da beispielsweise durch Stromausfälle oder Überflutungen (Wasser, Naturkatastrophen) die Produktion akut gefährdet sein kann.
  - spezifische Gefährdungen: auf das Unternehmen und den Standort bezogene spezifische Gefährdungen, die einen nennenswerten Schaden hervorrufen können

  B) Einstufung der Gefährdungen (Einschätzen und Bewerten) – (Kapitel 5 des BSI 200-3)

  - Einordnung der ermittelten Gefährdungen in vier Kategorien der **Eintrittshäufigkeit** (selten, mittel, häufig, sehr häufig)
  - Einordnung der ermittelten Gefährdungen in vier Kategorien der **Schadenshöhe** (vernachlässigbar, begrenzt, beträchtlich, existenzbedrohend)

[2] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

- Bestimmung von vier Risikokategorien und Beschreibung dieser, um die Gefährdungen individuell einstufen zu können (im Anschluss an diese Erklärung ist eine Beispielmatrix für die Risikoanalyse mit beispielhaften Definitionen der Risikokategorien dargestellt.)

C) Behandlung der Risiken (Vermeidung, Reduktion, Transfer und Akzeptanz) – (Kapitel 6 des BSI 200-3)

- Bestimmung von für das Unternehmen geeigneten Risikobehandlungsoptionen
- Vermeidung: Ist das Risiko durch eine Umstrukturierung eines Geschäftsprozesses vermeidbar?
- Reduktion: Sind weitere Maßnahmen zur Reduktion möglich und sinnvoll?
- Transfer: Kann das Risiko an einen externen Dienstleistenden ausgelagert werden? (Outsourcing oder Versicherungen)
- Akzeptanz: Ist es möglich, die potentiellen Konsequenzen des Risikos zu akzeptieren?

D) Konsolidierung des Sicherheitskonzepts (Integration in das Sicherheitskonzept) – (Kapitel 7 des BSI 200-3)

Zusätzliche Maßnahmen müssen anhand folgender Kriterien überprüft werden:

- Ist diese Maßnahme für den vorgesehenen Zweck geeignet und widerspricht nicht den Sicherheitszielen oder anderen Maßnahmen des Unternehmens?
- Ist die Maßnahme transparent und klar beschrieben, sodass der Inhalt für Mitarbeitende ersichtlich und verständlich ist?
- Ist die Maßnahme angemessen in Bezug auf die Gefährdung?
- Stehen Kosten, Aufwand und Nutzen im Gleichgewicht?

Für die Risikoanalyse kann der ausführliche Leitfaden im BSI-Standard 200-3 des Bundesamtes für Sicherheit in der Informationstechnik [14] sowie die vom BSI beispielhafte Ausführung einer Risikoanalyse anhand des fiktiven Unternehmens Recplast [13] genutzt werden.

Produzierende Unternehmen können unter Zuhilfenahme der DIN EN IEC 62443-3-2 [15] Maßnahmen zur Risikoreduzierung identifizieren und festlegen, die speziell für industrielle Automatisierungssysteme oder Produktionsanlagen relevant sind. Mithilfe dieser Norm werden entsprechende Security-Gegenmaßnahmen durch sog. Security-Levels in den einzelnen Produktionsbereichen (Zonen) festgelegt.

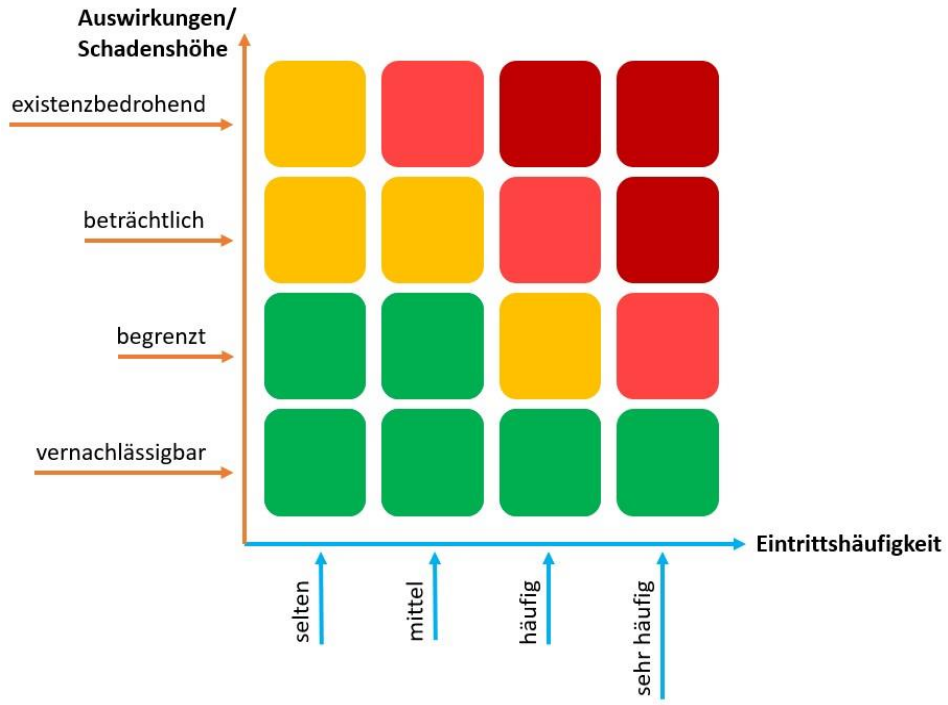

Abbildung 2: Beispiel einer Risikomatrix [6, S. 27]

Legende der Risikokategorien
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **einen** ausreichenden Schutz. **=> Aktuell keine Handlung oder Maßnahme notwendig**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **möglicherweise keinen** ausreichenden Schutz. **=> Beobachten und stetige Überprüfung der Maßnahmen**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **definitiv keinen** ausreichenden Schutz. **=> Handlungsbedarf, Neubewertung und regelmäßigere Überprüfung der Maßnahmen**
Bereits umgesetzte und vorgesehene Sicherheitsmaßnahmen bieten **definitiv keinen** ausreichenden Schutz. **=> Dringender Handlungsbedarf! Sofortige Neubewertung bestehender Schutzmaßnahmen/Umsetzung neuer Maßnahmen**

Abbildung 3: Legende zur Grafik aus Abbildung 2 [vgl. 6, S. 28]

Schritt 4: Organisation der IT-Sicherheit

Verantwortlichkeiten:

- Die Geschäftsleitung ist für alle Entscheidungen verantwortlich, sollte jedoch die Verantwortung an einzelne Personen delegieren.

Ziele:

- Aufbau einer IT-Organisation

Aktivität:

- Benennung des/der Verantwortliche(n) in der Geschäftsleitung und Dokumentation dieser.
- Zuweisen von
  - mindestens einer Person für die **IT-Verantwortung**.
  - mindestens einer Person als **Vertretung der Belegschaft** (ggf. aus dem **Betriebsrat**). [3]
  - mindestens einer Person für die **Administration der Systeme**. [4]
  - mindestens einer Person für den **Datenschutz** (**Datenschutzbeauftragte**). [3, 5]
  - einer Person für die Aufgaben der/s **Informationssicherheitsbeauftragen (ISB)** zu. [3]

[3] Bei kleinen und sehr kleinen Unternehmen, entfallen diese Positionen. Bei sehr kleinen Unternehmen ernennt die Geschäftsleitung **eine(n)** Mitarbeitende(n) zum/zur Informationssicherheitsverantwortlichen. Diese(r) ist für die gesamte Umsetzung der Maßnahmen verantwortlich.

[4] Bei sehr kleinen Unternehmen (< 10 Mitarbeitende) wird trotz der beschränkten Verfügbarkeit von Mitarbeitenden **empfohlen**, dass die Geschäftsleitung einen/eine Mitarbeitende(n) zum/zur **Systemadministrator**(in) ernennt, die geforderten technischen Maßnahmen für die Informationssicherheit zu implementieren und zu administrieren.

[5] Ein(e) Datenschutzbeauftragte(r) ist nur erforderlich, wenn im Unternehmen **dauerhaft** Mitarbeitende mit der Handhabung von personenbezogenen Daten beschäftigt sind [16].

Erläuterung der Aktivitäten:

Die Vertretungen der einzelnen genannten Bereiche bilden das **Informationssicherheits-team** (kurz IST). Die Aufgabe des IST besteht in der Unterstützung des/der ISB bei folgenden Tätigkeiten:

- Erkennen und Bewerten neuer Bedrohungen und Schwachstellen
- Entwickeln und Bewerten von Maßnahmen zur Informationssicherheit
- Steuern und Koordinieren der Maßnahmen zur Informationssicherheit (unternehmensweit)

Doppelbelegungen einer Funktion sollten möglichst vermieden werden. Sind Doppelbelegungen nicht zu vermeiden oder im Unternehmen sinnvoll, sollte die Begründung dokumentiert und zu den Akten genommen werden.

Dokumentation dieses Schrittes.

Das nachfolgende Organigramm zeigt den Aufbau der Informationssicherheit nach der Richtlinie VdS 10000 [6].

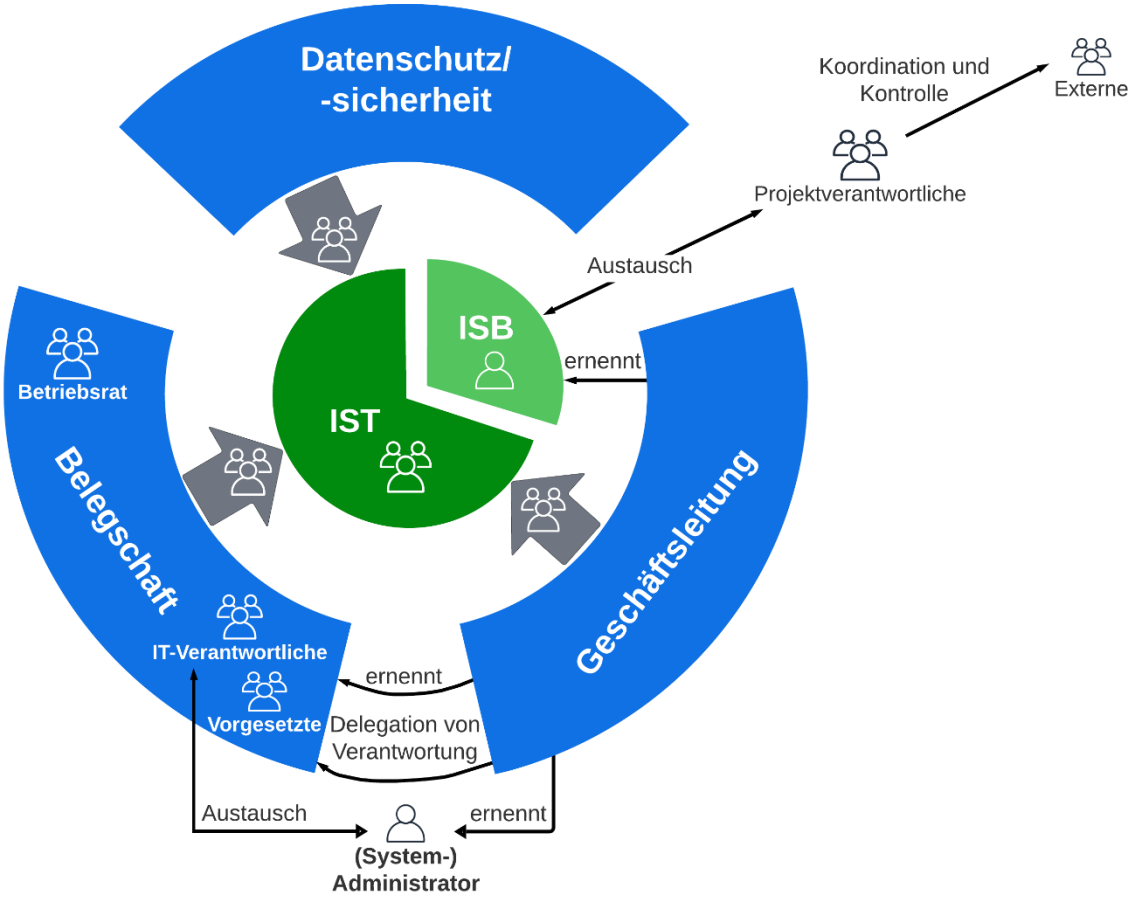

Abbildung 4: Organigramm der Informationssicherheit [17]

Schritt 5: Informationssicherheitsrichtlinien (ISR)

Eine Informationssicherheits**richt**linie ist ein unterstützendes Dokument der Informationssicherheits**leit**linie. In ihr werden weitergehende Regelungen für die Informationssicherheit getroffen und Maßnahmen dafür eingeführt.

Jede Richtlinie wird vom IST in Zusammenarbeit mit dem/der ISB erarbeitet und muss von der Geschäftsleitung in Kraft gesetzt werden.

Der/Die ISB ist verpflichtet, jede Richtlinie jährlich zu überprüfen und ggf. an die aktuellen Vorschriften (bspw. gesetzliche, vertragliche, behördliche) anzupassen.

Werden Änderungen an einer bestehenden Richtlinie vorgenommen oder wird eine neue Richtlinie erstellt, muss diese zeitnah den betreffenden Stakeholdern/Stakeholderinnen vorgelegt und ggf. verständlich erläutert werden.

Jede geltende Informationssicherheitsrichtlinie ist verpflichtend. Wird eine Richtlinie nicht mehr benötigt, muss diese durch die Geschäftsleitung aufgehoben werden.

Eine Richtlinie muss die folgenden Anforderungen erfüllen:

- Definition der Zielgruppe
  - Für wen ist diese Richtlinie handlungsweisend?
- Grund der Erstellung und Zielsetzung
  - Warum wird diese Richtlinie erstellt und was soll damit bezweckt werden?
- Kein Verstoß gegen die Leitlinien und Richtlinien des Unternehmens
- Kein Verstoß gegen andere Richtlinien, Gesetze oder Verordnungen
- Hinweis auf Nichtbeachtung
  - Was passiert, wenn die Richtlinie nicht eingehalten wird?
- Beschreibung von ggf. vorhandenen Ausnahmen
  - In Einzelfällen kann eine Richtlinie begründete Ausnahmen enthalten. Diese müssen jedoch genehmigt und dokumentiert werden.
- Verweis auf mitgeltende Unterlagen

Ist eine Informationssicherheitsrichtlinie aktiv, so gelten für die Zielgruppe dieser Richtlinie bestimmte Regelungen, die vorher von dem/der ISB festgelegt werden müssen.

Schritt 5.1: ISR – Mitarbeitende

Verantwortlichkeiten:

- Die Geschäftsleitung setzt diese ISR in Kraft und ist für die Einhaltung verantwortlich – kann diese Aufgabe jedoch delegieren.
- Die ISR wird von dem/der ISB in Zusammenarbeit mit dem IST entwickelt.

Ziele:

- Sicherstellung der Aufrechterhaltung der Informationssicherheit durch die Mitarbeitenden.

Aktivität:

- Vor Aufnahme der Tätigkeit von Mitarbeitenden
  - Überprüfung auf Eignung und Vertrauenswürdigkeit
- Bei Aufnahme der Tätigkeit von Mitarbeitenden
  - Schriftliche Erklärung zu Vertraulichkeit
  - Einweisung und Schulung in die Informationssicherheitsleitlinie und alle relevanten Reglungen
  - Freischaltung der erforderlichen IT-Ressourcen, Zugänge und Zugriffsrechte
  - Schulungen in Bezug auf die IT-Ressourcen
- Bei Beendigung oder Wechsel der Tätigkeit von Mitarbeitenden
  - Überprüfung und Anpassung der zur Verfügung gestellten IT-Ressourcen, Zugänge und Zugriffsrechte
  - In Kenntnis setzen aller relevanten Stakeholder/Stakeholderinnen über die Änderung

Erläuterung der Aktivitäten:

Für die Implementierung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems sind die Mitarbeitenden ein zentraler Faktor.

- Vor Aufnahme der Tätigkeit
  - Die angehenden Mitarbeitenden müssen vorab auf die Eignung und die Vertraulichkeit hin überprüft werden.
    Hierfür werden manchmal polizeiliche Führungszeugnisse angefragt.
- Bei Aufnahme der Tätigkeit
  - Die Mitarbeitenden müssen eine Vertraulichkeitsvereinbarung unterzeichnen, die sie zur Verschwiegenheit über unternehmensinterne Informationen verpflichtet. Diese Verschwiegenheitspflicht bleibt auch nach der Beendigung oder der Veränderung des Arbeitsverhältnisses bestehen.
  - Jeder/Jede Mitarbeitende muss bei Aufnahme der Tätigkeit über die Informationssicherheitsleitlinie des Unternehmens unterrichtet und im Umgang mit dieser geschult werden.
  - Für die Dauer des Arbeitsverhältnisses erhält der/die Mitarbeitende nur die im Rahmen seiner Tätigkeit erforderlichen IT-Ressourcen, Zugänge und Zugriffsrechte.
    Beispiele:
    - Ein(e) neue(r) Mitarbeitende(r) bekommt einen **Arbeitsplatz mit Computer** und die Zugangsinformationen und Zugriffsrechte für **Nutzende ohne administrative Rechte**.
    - Die Geschäftsleitung eines Unternehmens hat aufgrund ihrer Stellung hochrangige Zugriffsrechte, sollte aber dennoch nicht mit den administrativen Rechten ausgestattet sein. Dafür ist die Systemadministration zuständig.
  - Alle Mitarbeitenden müssen im Umgang mit den zu nutzenden IT-Ressourcen geschult werden.

    Beispiele:
    - Nur vom Unternehmen freigegebene Speicherorte dürfen für die dauerhafte Speicherung von Daten verwendet werden.
      (bspw. Netzwerklaufwerke)
    - Hard- und Software darf nicht von jedem/jeder Mitarbeitenden eigenmächtig verändert werden. (bspw. Umstecken von Bildschirmkabeln)
    - Netzwerkverbindungen (Zugänge zum Internet, VPN-Verbindungen, …) dürfen nicht eigenmächtig eingerichtet oder verändert werden.

  - Sicherheitsrelevante Einrichtungen und Maßnahmen dürfen nicht eigenmächtig deinstalliert, deaktiviert oder verändert werden.
    (bspw. Kensington-Schlösser, elektronische Schließmechanismen, …)
  - Die Verwendung von trivialen oder leicht zu entschlüsselnden Authentifizierungsmerkmalen ist untersagt.
    (bspw. Passwörter wie „Password“ oder „123456“)

  Über jede Regeländerung oder -erstellung müssen die Mitarbeitenden zeitnah unterrichtet und darin geschult werden.

  Laut der Cybersecurity Studie 2023 sind **55 % der Maßnahmen** nach einem IT-Sicherheitsvorfall **bessere bzw. intensivere** Schulungen der Mitarbeitenden [3, S. 19]!

- Bei Beendigung oder Wechsel der Tätigkeit
  - Bei Beendigung des Arbeitsverhältnisses oder Wechsel der Tätigkeit sind alle zugewiesenen IT-Ressourcen zu überprüfen und ggf. anzupassen.
    - Zugänge sind zu deaktivieren
      - Abgabe der Schlüssel und -karten
      - Abgabe des Unternehmensausweises
    - Zugriffsrechte sind zu entziehen
    - Abgabe von z. B. zur Verfügung gestellten Notebooks oder Tablets
    - Benutzerkonten sind zu löschen
    - gemeinsam genutzte Zugänge müssen neu eingerichtet bzw. die Authentifizierungsmerkmale verändert werden
  - In-Kenntnissetzen aller relevanten Stakeholder/Stakeholderinnen über die Änderung
    - Ein(e) Pförtner(in) sollte bspw. darüber informiert werden, dass ein(e) Mitarbeitende(r) nicht mehr für das Unternehmen arbeitet, damit dieser/diese nicht wie gewohnt das Gelände betreten kann.
  - Hierfür ist es bei einer Beendigung oder einem Wechsel des Beschäftigungsverhältnisses im Einvernehmen üblich, dass ein(e) Mitarbeitende(r) kurz vor Ende einen Laufzettel erhält, der aufzeigt welche Ressourcen er oder sie zurückgeben muss und welche Daten gesichert werden sollten.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 7** oder der **VdS 10005 Kapitel 6** nachgelesen werden.

Schritt 5.2: ISR – Wissen [6]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit den Vertretungen im IST ein Verfahren, um das Wissen in Bezug auf die Informationssicherheit aktuell zu halten, die Mitarbeitenden davon zu unterrichten und zu schulen.
- Die Geschäftsleitung ist dafür zuständig, dieses Verfahren in Kraft zu setzen.

Ziele:

- Das Unternehmen verfügt zu jedem Zeitpunkt über das aktuellste Wissen im Bereich der Informationssicherheit.
- Alle Mitarbeitenden verstehen ihre Verantwortlichkeiten und sind für ihre Tätigkeit geeignet und qualifiziert.

Aktivität:

- Implementierung eines Verfahrens, das bei einer Änderung der rechtlichen und technischen Bedingungen alle relevanten Stellen des Unternehmens und ggf. relevante externe Stellen in geeigneter Weise informiert.
- Implementierung eines Verfahrens zur Sensibilisierung und Schulung der Mitarbeitenden.

[6] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Für das Verfahren zur Mitteilung über geänderte rechtliche und technische Bedingungen muss folgendes gelten:
  - Es müssen regelmäßig aus verlässlichen Quellen Informationen (insb. akute Gefährdungen und mögliche Gegenmaßnahmen) über die technischen und rechtlichen Entwicklungen eingeholt werden.
    Verlässliche Quellen sind hierbei u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt/die Landeskriminalämter (BKA/LKÄ).
  - Die erhaltenen Informationen müssen unternehmensspezifisch ausgewertet und die betroffenen Bereiche ggf. angepasst werden.
  - Relevante Entwicklungen sind dem/der ISB und der Geschäftsleitung zeitnah mitzuteilen.
- Für das Verfahren zur Schulung und Sensibilisierung von Mitarbeitenden muss folgendes gelten:
  - Die Durchführung erfolgt regelmäßig und zusätzlich bei Bedarf.
  - Die Art und das Intervall müssen zielgruppenorientiert festgelegt werden.
  - Durch die Schulungen werden die Mitarbeitenden im Umgang mit den Inhalten der Informationssicherheitsleitlinie, der verschiedenen Informationssicherheitsrichtlinien und anderer relevanter Regelungen gestärkt.
  - In diesen Schulungen werden die Mitarbeitenden über die aktuellen Gefährdungen und das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen informiert und dadurch wird die Akzeptanz der Sicherheitsmaßnahmen bei der Belegschaft erhöht.
- Die Teilnahme der Mitarbeitenden sowie die Inhalte der Schulungen sollten dokumentiert werden.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 8** nachgelesen werden.

Schritt 5.3: ISR – Identifizieren kritische IT-Ressourcen [7]

Verantwortlichkeiten:

- Der/Die ISB ist für die Durchführung dieser Informationssicherheitsrichtlinie verantwortlich und verpflichtet, diese jährlich zu überprüfen.
- Die Geschäftsleitung muss diese ISR freigeben.

Ziele:

- Ermittlung und Identifikation der kritischen IT-Ressourcen des Unternehmens

Aktivität:

- Durchführung einer **Informationsklassifizierung** nach ISO/IEC 27001 [12]

  oder

- Durchführung einer **Schutzbedarfsanalyse** gemäß BSI-Standard 200-2 [18]

  oder

- andere Vorgehensweise

Erläuterung der Aktivitäten:

- Bei einer Schutzbedarfsanalyse werden die IT-Systeme, Örtlichkeiten, Anwendungen und Geschäftsprozesse auf ihren Schutzbedarf hin analysiert. Das BSI hat dafür am Beispiel des fiktiven Unternehmens *Recplast* eine Schutzbedarfsanalyse durchgeführt. Eine Schutzbedarfsfeststellung ähnlich der des Unternehmens Recplast sollte auf das eigene Unternehmen adaptiert werden.

Geschäftsprozesse

Kürzel	Titel	Beschreibung	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf
GP001	Produktion	Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis zur	Hoch Durch die Entwicklung von	Hoch Gefälschte oder falsche	Sehr Hoch Ein Ausfall
GP002	Angebotswesen	In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im	Hoch Es werden	Hoch Fehlerhafte Daten werden	Normal Ein Ausfall
GP003	Auftragsabwicklung	Kunden schicken die Bestellungen im Regelfall per Fax oder E-Mail. Zusätzlich bietet die	Hoch Es werden	Hoch Fehlerhafte oder manipulierte	Hoch Ein Ausfall
GP004	Einkauf	In der Einkaufsabteilung werden alle erforderlichen Artikel bestellt, die nicht für den	Hoch Es werden Verträge und	Normal Fehlerhafte Daten werden in	Normal Ein Ausfall
GP005	Disposition	In der Disposition werden alle für die Produktion benötigten Materialien (Kunststoffe, Schrauben,	Normal Es werden keine vertraulichen	Hoch Fehlerhafte Daten können zu	Hoch Ein Ausfall
GP006	Personalverwaltung	In dieser Abteilung werden alle Aufgaben bearbeitet, die zur administrativen Abwicklung	Hoch Es werden	Normal Fehlerhafte Daten können zu	Normal Ein Ausfall

Abbildung 5: Auszug aus der Schutzbedarfsfeststellung des BSI zu Recplast [7]

[7] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Schritt 5.4: ISR – IT-Systeme

Verantwortlichkeiten:

- Der/Die ISB entwickelt diese ISR in Zusammenarbeit mit dem IST.
- Die Geschäftsleitung ist für die Inkraftsetzung dieser ISR verantwortlich.

Ziele:

- Strukturierte Verwaltung der IT-Systeme und deren Absicherung.

Aktivität:

- Inventarisierung
  Implementierung eines Verfahrens zur Inventarisierung aller IT-Systeme im Unternehmen
- Basisschutz
  Jedes IT-System bedarf eines Basisschutzes gemäß **VdS 10000 Kapitel 10.3**.
- Lebenszyklus
  Ein IT-System besteht aus Hard- und Software. Für diese sog. Funktionseinheit müssen Verfahren implementiert werden, die diese Systeme von der Inbetriebnahme bis zur Ausmusterung begleiten.
- Zusätzliche Maßnahmen für mobile IT-Systeme
  Für mobile IT-Systeme im Unternehmensnetzwerk gelten besondere Sicherheitsmaßnahmen, da diese besonders der Gefahr von Diebstahl, unautorisiertem Zugriff oder unsicheren Netzwerken ausgesetzt sind.
  Für sie gelten die Regelungen, die in **Kapitel 10.4 der VdS 10000** beschrieben werden.
- Zusätzliche Maßnahmen für kritische IT-Systeme [8]
  Für alle kritischen IT-Systeme müssen zusätzlich die Regelungen gemäß **Kapitel 10.5 der VdS 10000** umgesetzt werden.

[8] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Inventarisierung

  Jedem IT-System, das inventarisiert wird, muss ein eindeutiges Identifizierungsmerkmal, ein Einsatzzweck und eine Lokalisierungsangabe (in der obigen Analogie: Straße und/oder Hausnummer) zugeordnet werden.

  Darüber hinaus wird empfohlen, dass noch weitere Informationen (Name, Versionen und Lizenzinformationen, installierte Software, Seriennummern, herstellendes Unternehmen, Garantieinformationen, Serviceverträge, …) erfasst werden.

- Basisschutz

  Hierzu zählen u. a. folgende Maßnahmen:

  - Maßnahmen zur Beschaffung von Software
    (z. B. vertrauenswürdige Quellen),
  - Maßnahmen zur Beschränkung des Netzwerkverkehrs
    (bspw. muss nicht jede/r Nutzende Zugriff auf das Archiv haben),
  - Maßnahmen zur Protokollierung von Ereignissen
    (gescheiterte/erfolgreiche Anmeldeversuche, Fehlercodes, sonstige Ereignisse),
  - Maßnahmen zum Schutz vor Schadsoftware u. v. m.
    Hierbei ist darauf zu achten, dass ein produzierender Bereich eines Unternehmens besonders geschützt werden muss, da ein Echtzeit-Schutz während der laufenden Produktion oftmals nicht möglich ist.

  Das Implementieren eines Basisschutzes für ein IT-System umfasst sehr viele einzelne Maßnahmen, deren Beschreibung in diesem Leitfaden zu umfangreich wären und deshalb in der **VdS 10000 Kapitel 10.3** nachgelesen werden können.

- Lebenszyklus

  Es ist für jedes der beiden Stadien eines IT-Systems (Inbetriebnahme/Änderung und Ausmusterung/Wiederverwendung) ein Verfahren zur Überprüfung zu integrieren.

  Inbetriebnahme/Änderung:

  - Ist das IT-System systemkritisch? Ist der Basisschutz umgesetzt?
  - Aktualisierung des Netzwerkplans und der Inventarisierung
  - Dokumentation der Arbeitsschritte

  Ausmusterung/Wiederverwendung

  - Sicherung bzw. Archivierung der Daten
  - Schutz der Daten vor unberechtigtem Zugriff (ggf. Löschung der Daten)
  - Aktualisierung des Netzwerkplans und der Inventarisierung
  - Dokumentation der Arbeitsschritte

- Zusätzliche Maßnahmen für mobile IT-Systeme
  Beispielhafte Maßnahmen sind:

  - Mobile IT-Systeme dürfen bei Verlust oder Beschädigungen keine Informationen an Dritte preisgeben.
  - Vorabdefinition von Verhaltensweisen in Bezug auf das mobile IT-System.

  Es gibt zahlreiche Maßnahmen für mobile IT-Systeme, deren Beschreibung in diesem Leitfaden zu weit gehen würden und deshalb in der **VdS 10000 Kapitel 10.4** nachgelesen werden können.

- Zusätzliche Maßnahmen für kritische IT-Systeme

  - Ein Unternehmen sollte für jedes kritische IT-System ein Notbetriebsniveau implementieren und ein passendes Ersatzsystem verfügbar halten.
  - Regelmäßige Updates sollten vorher auf einem vergleichbaren System getestet werden. Dies ist explizit für den produzierenden Bereich eines Unternehmens wichtig, da eine fehlerhafte Software sehr schnell zu einem Totalausfall im Unternehmen führen kann.
  - Kritische IT-Systeme sollten dauerhaft überwacht werden.

  Es gibt zahlreiche Maßnahmen für kritische IT-Systeme, deren Beschreibung in diesem Leitfaden zu weit gehen würden und deshalb in der **VdS 10000 Kapitel 10.5** nachgelesen werden können.

Genauere Informationen zu dieser ISR sind in der **VdS 10000 Kapitel 10** beschrieben.

Schritt 5.5: ISR – Netzwerke und Verbindungen

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die Inkraftsetzung dieser verantwortlich.

Ziele:

- Abgesicherte Kommunikation über alle Netzwerke (intern und extern) hinweg

Aktivität:

- Netzübergänge sichern
- Implementierung eines Basisschutzes für Netzwerke
- Risikoanalyse für kritische Verbindungen

Erläuterung der Aktivitäten:

- Die Informationssicherheitsrichtlinie muss für jeden Netzübergang zu weniger stark gesicherten Netzwerken angewendet werden.
  - Beschränkung des Netzwerkverkehrs auf das funktionale Minimum
  - Untersuchung und ggf. Blockierung von Schadsoftware
  - Behandlung von Schadsoftware als Sicherheitsvorfall
  - Jährliche Überprüfung der Konfiguration aller Netzwerkkomponenten
- Implementierung eines Basisschutzes für Netzwerke
  - Nicht dauerhaft genutzte Netzwerkanschlüsse müssen vor unberechtigter Nutzung gesichert werden.
  - Prüfung, ob eine Segmentierung des Unternehmensnetzwerkes möglich ist.
  - Absicherung der Daten vor Fernzugriffen (z. B. für Wartung) und bei Netzwerkkopplungen bzgl. der Schutzziele Vertraulichkeit, Integrität und Authentizität (z.B. durch anerkannte Sicherheitsstandards wie VPN, ZTNA, SD-WAN, …)
  - Absicherung des WLAN vor Fernzugriffen durch anerkannte Standards (WPA2, WPA3, …)
- Die Risikoanalyse für die kritischen Netzwerkverbindungen ist nach anerkannten Standards (z. B. BSI Standard 200-3 [14]) auszuführen.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 11** oder der **VdS 10005 Kapitel 8** nachgelesen werden.

Schritt 5.6: ISR – Mobile Datenträger [9]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die Umsetzung und die Inkraftsetzung dieser verantwortlich.

Ziele:

- Sicherer Umgang mit mobilen Datenträgern in Bezug auf die Informationssicherheit

Aktivität:

- Bestimmung der Daten, die auf einem mobilen Datenträger gespeichert werden dürfen
- Information der Mitarbeitenden und Nutzenden über die spezifischen Risiken und Gefahren (Diebstahl, Verlust, Einschleppen von Schadsoftware) im Umgang mit mobilen Datenträgern
- Mobile Datenträger mit Unternehmensdaten sind vertraulich zu behandeln
- Schutz der Daten durch geeignete und anerkannte Verschlüsselungsverfahren
- Risikoanalyse für kritische mobile Datenträger

[9] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Bestimmung der Daten, die auf einem mobilen Datenträger gespeichert werden dürfen
  - Daten, die besonders geschützt werden sollten, weil sie beispielsweise personenbezogene Daten oder besonders schützenswerte Unternehmensgeheimnisse enthalten, sollten nicht auf mobilen Datenträgern gespeichert werden.
  - Sollte dies jedoch notwendig sein, sollten diese Daten verschlüsselt werden, sodass keine dritte Partei bei Diebstahl oder Verlust Zugriff auf diese Daten erhalten kann.
- Information der Mitarbeitenden und Nutzenden über die spezifischen Risiken und Gefahren (Diebstahl, Verlust, Einschleppen von Schadsoftware) im Umgang mit mobilen Datenträgern
  - Arbeits-USB-Sticks, auf denen z. B. eine Präsentation gespeichert wurde und die an einem fremden IT-System angeschlossen war, kann von diesem IT-System Schadsoftware übernommen haben. Es ist unbedingt zu vermeiden, dass solche und andere potentiell infizierte Datenträger Zugang zum Unternehmensnetzwerk erhalten.
  - Sind auf einem mobilen Datenträger z. B. die Mischungsverhältnisse von vom Unternehmen entwickelten Stoffen enthalten, sind diese für die Konkurrenz des eigenen Unternehmens von besonderem Interesse.
- Mobile Datenträger mit Unternehmensdaten sind vertraulich zu behandeln
  - Unternehmensdaten umfassen alle Daten, die einen Rückschluss auf das Unternehmen ermöglichen.
- Schutz der Daten durch geeignete und anerkannte Verschlüsselungsverfahren
- Risikoanalyse [14] für kritische mobile Datenträger

Laut den Befragten der Cybersecurity Studie 2023 birgt die private Nutzung von Firmengeräten erhebliche Gefahren. [3, S. 29]

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 12** nachgelesen werden.

Schritt 5.7: ISR – Umgebung/Umwelteinflüsse

Verantwortlichkeiten:

- Die Geschäftsleitung ist dazu verpflichtet, das Unternehmen gegen negative Umwelteinflüsse abzusichern.

Ziele:

- Schutz von Servern, aktiven Netzwerkkomponenten, Netzwerkverteilstellen und Datenleitungen gegenüber äußeren negativen Einflüssen.

Aktivität:

- Die Entwicklung der ISR sollte mithilfe eines anerkannten Standards (z. B. VdS 2007 [19]) erfolgen.

Erläuterung der Aktivitäten:

- In dem Standard VdS 2007 [19] werden potentielle Gefahren von außerhalb und dazugehörige mögliche Schutzmaßnahmen aufgezeigt. Ebenfalls sind hierin Tabellen enthalten, die eine Schutzbedarfsanalyse mit dazugehörigen Maßnahmen enthalten.
- Eine Möglichkeit, ein Unternehmen zu schützen, zeigt das sog. „Defence in Depths“-Konzept. Bei diesem Konzept wird die Sicherung des Unternehmens ähnlich einer Zwiebel aufgebaut. Jede Zwiebelschicht steht sinnbedeutend für eine Verteidigungslinie (z. B. Firewall) nach außen hin. Die äußerste Schale stellt z. B. ein umgebender Zaun dar. Näher Informationen zu diesem Konzept sind im ersten Bereich der DIN EN IEC 62443 [20] Normenreihe zu finden.
- Da der Standard frei verfügbar ist, wird in diesem Leitfaden auf eine detaillierte Darstellung verzichtet und lediglich auf den Standard verwiesen.

Wird ein anderer Standard als die **VdS 2007** zur Entwicklung der ISR gewählt, so sind die Anforderungen aus **VdS 10000 Kapitel 13** oder aus **VdS 10005 Kapitel 9** zu erfüllen. Genauere Informationen zu dieser ISR können dort ebenfalls nachgelesen werden.

Schritt 5.8: ISR – IT-Outsourcing und Cloud-Computing

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Unternehmensleitung ist für die Inkraftsetzung dieser verantwortlich.
- Die Unternehmensleitung ist zusätzlich für die Einhaltung der Verträge mit externen Dienstleistenden und die Gestaltung der Verträge zuständig.
- Die Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Delegation von Verantwortung an externe Unternehmen
- Wahrung der IT-Sicherheitsinteressen des Unternehmens
- Einsparung von materiellen und/oder personellen Ressourcen

Aktivität:

- Jedes Vorhaben, Aspekte der IT des Unternehmens auszulagern, muss dokumentiert werden.
- Das Unternehmen und die Mitarbeitenden müssen über die Auslagerung von IT-Ressourcen informiert und auf diese vorbereitet bzw. im Umgang damit geschult werden.
- Die Verträge müssen so gestaltet werden, dass das anbietende Unternehmen sämtliche Anforderungen bzgl. der IT-Sicherheitsinteressen des eigenen Unternehmens erfüllt.

Erläuterung der Aktivitäten:

- Für jedes Vorhaben, Aspekte der IT des Unternehmens auszulagern, müssen folgende Punkte zwingend dokumentiert werden:
  - Welche IT-Ressourcen werden ausgelagert?
  - Müssen betriebliche, gesetzliche und vertragliche Bestimmungen insbesondere in Bezug auf die drei Hauptschutzziele Vertraulichkeit, Integrität und Verfügbarkeit beachtet werden?
  - Ist die auszulagernde IT-Ressource eine kritische IT-Ressource?
- Das Unternehmen und die Mitarbeitenden müssen über die Auslagerung von IT-Ressourcen informiert und auf diese vorbereitet bzw. im Umgang damit geschult werden.
- Die Verträge müssen so gestaltet werden, dass das anbietende Unternehmen sämtliche Anforderungen bzgl. der IT-Sicherheitsinteressen des eigenen Unternehmens erfüllt.
  - Ansprüche aus Vertragsverletzungen gegen das anbietende Unternehmen können auch durchgesetzt werden, wenn dieses sich nicht im selben Rechtsraum befindet.
  - Bei einer Beendigung des Vertrages (Insolvenz oder Auflösung) wird vereinbart, dass sämtliche IT-Ressourcen in Bezug auf das Unternehmen herausgegeben werden müssen.
  - Weiterhin wird vereinbart, dass bei Beendigung des Vertrages das ehemalige anbietende Unternehmen den Migrationsprozess zum neuen Anbieter unterstützen muss.
  - Einhaltung der Datenschutzbestimmungen gemäß VdS 10010

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 14** oder der **VdS 10005 Kapitel 11** nachgelesen werden.

Schritt 5.9: ISR – Zugänge und Zugriffsrechte [10]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Mithilfe der Zugänge und Zugriffsrechte wird der Zugang zu den internen IT-Ressourcen gewährt. Diese müssen vor unberechtigtem Zugriff geschützt werden.

Aktivität:

- Implementierung von Verfahren zum Anlegen, Ändern und Zurücksetzen von Zugängen und Zugriffsrechten
- Jährliche Überprüfung der Zugänge und Zugriffsrechte zu kritischen IT-Ressourcen.

[10] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Implementierung von Verfahren zum Anlegen, Ändern und Zurücksetzen von Zugängen und Zugriffsrechten
  - Jeder Vorgang muss beantragt, geprüft und von der/dem ISB genehmigt werden.
  - Genehmigungen werden nur erteilt, wenn diese für die Aufgabenerfüllung des/der Nutzenden notwendig sind.
  - Administrative Zugänge und Zugriffsrechte bedürfen besonderen Begründungen.
  - Antragsstellende (meist die Nutzenden) müssen zeitnah über das Anlegen und Ändern informiert werden. Auf die Information beim Löschen kann verzichtet werden.
  - Alle Vorgänge müssen ausführlich dokumentiert werden.
- Jährliche Überprüfung der Zugänge und Zugriffsrechte zu kritischen IT-Ressourcen.
  - Jährliche Erfassung und Überprüfung aller Zugänge und Zugriffsrechte bei kritischen IT-Ressourcen
  - Nicht (mehr) benötigte Zugänge und Zugriffsrechte sind zu entfernen
  - Nicht ordnungsgemäß angelegte Zugänge sind als Sicherheitsvorfall (Schritt 5.12) zu betrachten.

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 15** nachgelesen werden.

Schritt 5.10: ISR – Datensicherung und -archivierung

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die ggf. vorhandene Administration ist für die technische Umsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Absicherung der Verfügbarkeit der Daten durch Datensicherungs- und -archivierungsverfahren, da unbrauchbare oder verlorene Daten nicht entsetzt werden können.

Aktivität:

- Festlegung der Speicherorte
- Archivierung ausgewählter Daten, um betrieblichen, gesetzlichen und vertraglichen Anforderungen zu genügen
- Implementierung von Verfahren zur Datensicherung, -archivierung und -wiederherstellung
- Jährliche Überprüfung der Datensicherungen und Archivierungen
- Implementierung eines Basisschutzes für jeden Speicherort und jedes IT-System
- Besondere Verfahren bei kritischen IT-Systemen
- Implementierung von Wiederanlaufplänen

Erläuterung der Aktivitäten:

- Die Speicherorte sollten unter Zuhilfenahme der **3**-**2**-**1**-Methode gewählt werden. Diese Methode sieht vor, dass **drei** Datenkopien erstellt werden.

  Zwei Datenkopien werden auf verschiedenen Speichermedien und **die dritte Datenkopie** an einem anderen Ort aufbewahrt.

- Viele Daten müssen aufgrund von betrieblichen, gesetzlichen und vertraglichen Auflagen für einen bestimmte Zeitraum zur Verfügung stehen und sollten daher archiviert werden. Der Basisschutz für einen Speicherort kann äquivalent zu dem eines IT-Systems aus Schritt 5.4 aufgebaut werden.
- Die Vorgaben der VdS-Richtlinien hierzu sind sehr umfangreich und übersteigen den Rahmen dieses Leitfadens. Nachzulesen sind alle genannten Punkte in der
  - **VdS 10000 Kapitel 16** für kleine und mittlere Unternehmen

    oder der
  - **VdS 10005 Kapitel 10** für kleine und sehr kleine Unternehmen.

Schritt 5.11: ISR – Störungen und Ausfälle [11]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.
- Die (System-)Administration ist für die technische Instandsetzung und die technische Verwaltung der ISR zuständig.

Ziele:

- Zügige Rückkehr zum Regelbetrieb und Schadensminimierung nach Störung oder Ausfall

Aktivität:

- Implementierung eines Business Continuity Managements (BCM) nach anerkanntem **BSI Standard 200-4** [21] oder **DIN EN ISO 22301** [22].

[11] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Ein Business Continuity Management ist im Grunde das Notfall- bzw. Krisenmanagement des Unternehmens. Hierbei werden verschiedene Bereiche abgedeckt:
  - IT-/System-Ausfall
  - Gebäudeausfall
  - Ausfall von Dienstleistenden
- Für ein einfaches Notfallmanagement sollten folgende Punkte bedacht werden:
  - Bestimmung eines/r **IT-Notfall-Beauftragten**, der/die im Falle eines Notfalls sofort und zu jedem Zeitpunkt kontaktiert werden kann.
  - Erstellen oder Ausfüllen einer **IT-Notfallkarte** (ähnlich zu den Notfallkarten in einem Flugzeug), damit die Mitarbeitenden informiert sind und wissen, was bei einem Notfall zu tun ist. Diese sollte jedem/jeder Mitarbeitenden in einer offline-Version zur Verfügung stehen.
    Diese Notfallkarte sollte die Erreichbarkeit der/s **IT-Notfall-Beauftragten** sowie das Verhalten während eines Notfalls enthalten.
  - Während des Notfalls sollten alle Sachverhalte genauestens dokumentiert werden.

Abbildung 6: Beispielhafte Notfallkarte [14]

Wird eine andere Vorgehensweise gewählt oder sind genauere Informationen erwünscht, so sind die Anforderungen an diese ISR in der **VdS 10000 Kapitel 17** oder dem **BSI Standard BSI 200-4** [21] nachzulesen.

Schritt 5.12: ISR – Sicherheitsvorfälle [12]

Verantwortlichkeiten:

- Der/Die ISB entwickelt in Zusammenarbeit mit dem IST diese ISR.
- Die Geschäftsleitung ist für die verwaltungstechnische Umsetzung und die Inkraftsetzung der ISR verantwortlich.

Ziele:

- Schnelle Eindämmung und Behebung von Schäden

Aktivität:

- Treffen von Regelungen für den Umgang mit IT-Sicherheitsvorfällen
- Implementierung von Maßnahmen zur Erkennung
- Implementierung eines Verfahrens zur zeitnahen Reaktion

[12] Für kleine und sehr kleine Unternehmen ist dieser Vorgang für eine Zertifizierung in den VdS-Richtlinien nicht vorgeschrieben.

Erläuterung der Aktivitäten:

- Treffen von Regelungen für den Umgang mit IT-Sicherheitsvorfällen
  - Definition des Begriffes „Sicherheitsvorfall“.
  - Jedem/r Mitarbeitenden sollte es erlaubt und möglich sein, Sicherheitsvorfälle zu melden (positive Fehlerkultur/anonyme Meldewege).
  - Definition der Art der Kommunikation (auch gegenüber der Geschäftsleitung) über diesen Sicherheitsvorfall.
  - Sicherheitsvorfälle sind von der/dem ISB vorrangig zu bearbeiten.
- Implementierung von Maßnahmen zur Erkennung
  - Implementierung von Angriffserkennungssystemen im Unternehmensnetzwerk (bspw. Prüfsummen zur Integritätsprüfung, sog. Honeypots, usw.)
- Implementierung eines Verfahrens zur zeitnahen Reaktion
  1. Schnelle Übersichtgewinnung und ggfs. Schutz von Personen
  2. Schadenseindämmung und -dokumentation
  3. Beweissicherung
  4. Schadensbehebung & Wiederanlauf
  5. Nachbereitung/Verbesserungen

Genauere Informationen zu dieser ISR können in der **VdS 10000 Kapitel 18** nachgelesen werden.

5 Leitfaden zur Einführung eines ISMS bei KMU – Abschluss

Wenn die vorangegangenen Schritte durchgeführt wurden, wurde ein Informationssicherheitsmanagementsystem passend zu dem Unternehmen in den Unternehmensablauf integriert. Ein solches Managementsystem muss jedoch regelmäßig an sich ändernde Regularien und Vorschriften angepasst werden. Hierfür sollten in regelmäßigen Abständen (ungefähr jährlich) die eben getroffenen Entscheidungen und Maßnahmen überprüft und ggf. an die geänderten Rahmenbedingungen angepasst werden.

Wenn größere Änderungen im Unternehmen vorgenommen werden (z. B. Abteilungen eröffnen oder schließen, Standorte eröffnen oder schließen, usw.), kann es erforderlich werden, das ISMS auch vor Ablauf eines Jahres grundlegend anzupassen.

Abschließend ist noch zu erwähnen, dass laut der anfangs erwähnten TÜV-Studie die Ausgaben in Bezug auf die Informationssicherheit in KMU in den letzten zwei Jahren bei etwa der Hälfte der kleinen und bei etwa 2/3 der mittleren Unternehmen gestiegen sind. Der Trend zeigt, dass immer mehr Unternehmen in die Informationssicherheit investieren (Abbildung 7) [2].

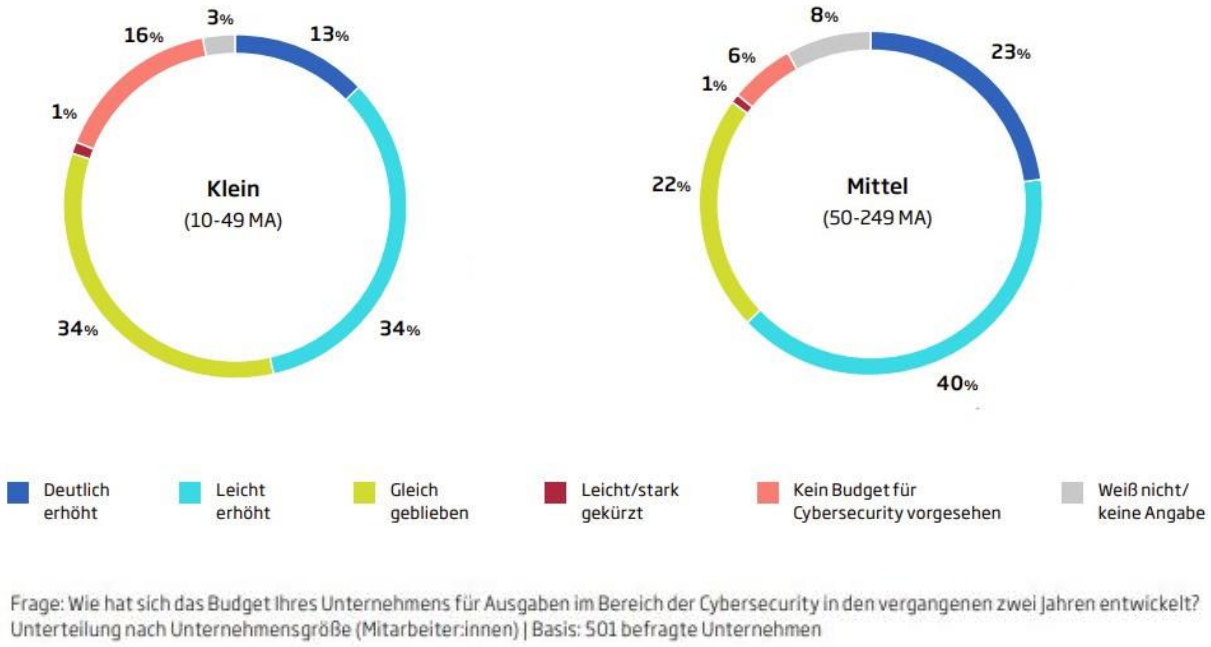

Abbildung 7: Entwicklung der Ausgaben für Cybersecurity [3, S. 34]

Dieser Leitfaden ist ein Instrument, das in den Ablauf des Unternehmens integriert und Teil des Informationssicherheitfortschritts der KMU in Deutschland [3, S. 34] sein sollte. Auch wenn die Kosten für die zusätzlichen Maßnahmen teilweise hoch sein mögen, sagen etwa ⅔ der Unternehmen, dass das Verhältnis zwischen eingesetzten Ressourcen und dem Sicherheitsgewinn ausgeglichen ist [3, S. 39].

6 Abbildungsverzeichnis

Abbildung 1: Bedeutung der Cybersecurity in Unternehmen [1, S. 8] 1
Abbildung 2: Beispiel einer Risikomatrix [6, S. 27] 13
Abbildung 3: Legende zur Grafik aus Abbildung 2 [vgl. 6, S. 28] 13
Abbildung 4: Organigramm der Informationssicherheit [17] 15
Abbildung 5: Auszug aus der Schutzbedarfsfeststellung des BSI zu Recplast [7] 22
Abbildung 6: Beispielhafte Notfallkarte [14] 37
Abbildung 7: Entwicklung der Ausgaben für Cybersecurity [3, S. 34] 40

7 Abkürzungsverzeichnis/Glossar

Deutsch	Beschreibung
Bedrohung	Durch Schwachstellen ausgelöste potentielle Gefahren werden als Bedrohung angesehen. Wird z.B. der Informationsgehalt einer Nachricht ausspioniert („Man-In-The-Middle“ – Angriff) oder manipuliert, handelt es sich um eine Bedrohung für die beiden Kommunikationspartner. Bedrohungen können darüber hinaus von der Technik (z.B. Kabelbrand), durch eine Fehlbedienung eines Mitarbeitenden (z.B. Überfahren eines Stop-Signals) oder durch das Anwenden von Gewalt ausgehen.
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
Cyberangriff	Von außen (durch einen einzelnen Hacker, durch eine Institution o. ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff auf ein Computernetzwerk [23]
DIN	**D**eutsches **I**nstitut für **N**ormung
EN	**E**uropäische **N**orm
Echtzeitschutz	Ein Echtzeitschutz überwacht das System permanent in Echtzeit und schützt jederzeit zuverlässig vor Infektionen. Er läuft automatisch im Hintergrund und überwacht das System kontinuierlich vgl. [24].
IEC	Internationale Elektrotechnische Kommission (**I**nternational **E**lectrotechnical **C**ommission)
ISO	Internationale Organisation für Normung (**I**nternational **O**rganization for **S**tandardization)
KMU	**K**leine (und sehr kleine) und **m**ittlere **U**nternehmen mit weniger als 250 Mitarbeitenden [25] • **sehr kleine** Unternehmen: weniger als **zehn** Mitarbeitende maximale Jahresbilanzsumme von **zwei** Mio. Euro

	• **kleine** Unternehmen: weniger als **50** Mitarbeitende maximale Jahresbilanzsumme von **zehn** Mio. Euro • **mittlere** Unternehmen: weniger als **250** Mitarbeitende maximale Jahresbilanzsumme von **43** Millionen Euro
KRITIS	Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. [26] (Bspw. Klärwerke, Energieversorger, Atomkraftwerke, Chemiekonzerne)
Leitfaden	Kurze, übersichtliche und gut verständliche Handlungsanweisung mit einem leicht bindenden Charakter [27]
Geschäftsleitung	• Oberste Leitungsebene in einem Unternehmen • geschäftsführende Direktion • Inhaber(in) oder Geschäftsführung bei kleineren Unternehmen
Man-In-The-Middle - Angriff	Bei einem „Man-in-the-Middle“-Angriff schaltet sich eine fremde Partei in eine bestehende Kommunikation ein, hört diese – meist unbemerkt – ab und ist in der Lage die Daten zu manipulieren. [28]
Norm	Dokument, das Regeln, Leitlinien oder Merkmale für Tätigkeiten festlegt [29]
Richtlinie	Eine Richtlinie ist eine Handlungs- oder Ausführungsvorschrift einer Institution oder Instanz, die jedoch kein förmliches Gesetz ist. [30]
Risiko	Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit und Ausmaß eines Schadens. Als Risiko werden Szenarien beschrieben, die eine Relevanz für den vorliegenden Fall darstellen [31, S. 33]. Risiken sind das Zusammenspiel aus Assets, Schwachstellen und daraus resultierenden Bedrohungen.

Schwachstelle	Eine Schwachstelle ist eine Lücke in der Informationssicherheit. Sie stellt eine Bedrohung dar, da hierdurch Unbefugten der Zugang zu Systemressourcen und vertraulichen Daten möglich ist. Die Ursachen für die Schwachstelle können in der Konzeption, der verwendeten Algorithmen, der Implementation, der Konfiguration oder dem Betrieb sowie dem Unternehmen liegen [31, S. 33].

Stakeholder/ Stakeholderinnen	Gruppe von Personen, die ein berechtigtes Interesse an der Entwicklung eines Unternehmens haben [32]
	• interne Stakeholder/Stakeholderinnen
	  ○ Mitarbeitende
	  ○ Manager/Managerinnen
	  ○ Eigentümer/Eigentümerinnen
	• externe Stakeholder/Stakeholderinnen
	  ○ Lieferanten/Lieferantinnen
	  ○ Kunden/Kundinnen
	  ○ Gläubiger/Gläubigerinnen

VdS	Ehemals „**V**erband **d**er **S**achversicherer“, heute 100%ige Tochter der „Deutschen Versicherungswirtschaft“ (GDV) [33]
VPN	**V**irtual **P**rivate **N**etwork
ZTNA	**Z**ero **T**rust **N**etwork **A**ccess (Alternative zum VPN) [34]
SD-WAN	**S**oftware-**D**efined – **W**ide **A**rea **N**etwork [35]
WPA2/WPA3	Wi-Fi Protected Access 2/3

8 Literatur

[1] ZDNet-Redaktion. „Jedes 10. Unternehmen Opfer eines Hackerangriffs: Cybersecurity-Studie TÜV-Verband: Phishing und Erpressungssoftware häufigste Angriffsmethoden / Cyber Resilience Act zügig verabschieden." https://www.zdnet.de/88409783/1-von-10-unternehmen-im-jahr-2022-opfer-eines-hackerangriffs/ (Zugriff am: 18. Juni 2023).

[2] Maurice Shahd. „TÜV Cybersecuritystudie 2023." https://www.tuev-verband.de/studien/cybersicherheit-in-deutschen-unternehmen (Zugriff am: 18. Juni 2023).

[3] Dr. Johannes Bussmann, Dr. Gerhard Schabhüser. „Cybersicherheit in deutschen Unternehmen: TÜV Cybersecurity Studie 2023." https://www.tuev-verband.de/?tx_epxelo_file[id]=925194&cHash=11772152e3b993dd496a49e3e533076f (Zugriff am: 18. Juni 2023).

[4] ISACA Germany Chapter e.V. „Implementierungsleitfaden ISO/IEC 27001:2013: Ein Praxisleitfaden für die Implementierung eines ISMS nach ISO/IEC 27001:2013." https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf (Zugriff am: 18. Juni 2023).

[5] WissenHoch2, *Cybercrime: Wie können wir uns schützen?* Zugriff am: 15. Juni 2023. [Online]. Verfügbar unter: https://www.3sat.de/wissen/wissenschaftsdoku/230615-sendung-cybercrime-wido-100.html

[6] *VdS 10000 - Informationssicherheits-Managementsystem für kleine und mittlere Unternehmen (KMU),* VdS Schadenverhütung GmbH.

[7] *VdS 10005 - Mindestanforderungen an die IT-Sicherheit für Klein- und Kleinstunternehmen,* VdS Schadenverhütung GmbH.

[8] *DIN SPEC 27076:2023-05, IT-Sicherheitsberatung für Klein- und Kleinstunternehmen,* DIN, Berlin.

[9] Europäische Kommission, *https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act*, 2023. Zugriff am: 19. Juli 2023. [Online]. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[10] Bundesamt für Sicherheit in der Informationstechnik. „Informationen zur Wahl des Geltungsbereiches." https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-Nachweise/Wahl-des-Geltungsbereiches/wahl-des-geltungsbereiches_node.html (Zugriff am: 18. Juni 2023).

[11] *DIN ISO 31000:2018-10, Risikomanagement_ - Leitlinien (ISO_31000:2018),* DIN, Berlin.

[12] *DIN EN ISO/IEC 27001:2017-06, Informationstechnik_ - Sicherheitsverfahren_ - Informationssicherheitsmanagementsysteme_ - Anforderungen (ISO/IEC_27001:2013 einschließlich Cor_1:2014 und Cor_2:2015); Deutsche Fassung EN_ISO/IEC_27001:2017,* DIN, Berlin.

[13] Bundesamt für Sicherheit in der Informationstechnik. „Arbeitsbeispiel RECPLAST GmbH." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/

Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Hilfsmittel-und-Anwenderbeitraege/Recplast/Recplast.html (Zugriff am: 18. Juni 2023).

[14] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-3 - Risikomanagement." https://www.bsi.bund.de/dok/10027822 (Zugriff am: 18. Juni 2023).

[15] *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung*, DIN EN IEC 62443-3-2:2021-12, DIN, Dez. 2021. [Online]. Verfügbar unter: https://www.beuth.de/de/norm/din-en-iec-62443-3-2/344299957

[16] Europäische Kommission. „Gelten die Vorschriften für KMU?: Datenschutz-Grundverordnung bei KMU." https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_de (Zugriff am: 19. Juli 2023).

[17] Marian Thöne, *Organigramm eines Informationssicherheitsteams: - Eigene Entwicklung eines Schaubildes*, 2023.

[18] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-2 - IT-Grundschutz-Methodik." https://www.bsi.bund.de/dok/10027846 (Zugriff am: 18. Juni 2023).

[19] *VdS 2007 : 2016-03 - Informationstechnologie (IT-Anlagen) – Gefahren und Schutzmaßnahmen,* VdS Schadenverhütung GmbH.

[20] *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber*, IEC 62443-2-1, DIN, Sep. 2020. [Online]. Verfügbar unter: https://www.beuth.de/de/norm-entwurf/din-en-iec-62443-2-1/327919389

[21] Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-4 - Business Continuity Management: Community Draft." https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (Zugriff am: 18. Juni 2023).

[22] *DIN EN ISO 22301:2020-06, Sicherheit und Resilienz_- Business Continuity Management System_- Anforderungen (ISO_22301:2019); Deutsche Fassung EN_ISO_22301:2019,* DIN, Berlin.

[23] DUDEN. „Cy-ber-at-ta-cke, die." https://www.duden.de/rechtschreibung/Cyberattacke (Zugriff am: 19. Juni 2023).

[24] Avira. „Was ist der Unterschied zwischen Echtzeitschutz und System-Scanner?" https://support.avira.com/hc/de/articles/360000153538-Was-ist-der-Unterschied-zwischen-Echtzeitschutz-und-System-Scanner- (Zugriff am: 20. Juni 2023).

[25] Europäische Kommission, *Definition der Kleinstunternehmen sowie der kleinen und mittleren Un-ternehmen.* Zugriff am: 22. Februar 2023. [Online]. Verfügbar unter: http://data.europa.eu/eli/reco/2003/361/oj

[26] Bundesamt für Sicherheit in der Informationstechnik. „Was sind Kritische Infrastrukturen?: Definition KRITIS." https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-

Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (Zugriff am: 19. Juni 2023).

[27] Dipl. Päd. Uta Reimann-Höhn. „Einen Leitfaden erstellen - Erklärung und Beispiele." https://reimann-hoehn.de/der-leitfaden-erklaerung-und-beispiel/ (Zugriff am: 18. Juni 2023).

[28] Bundesamt für Sicherheit in der Informationstechnik. „Man-In-The-Middle-Angriff." https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html

[29] Stephan Baumann. „Definition Normen - Standards: Normen." https://www.ihk.de/koblenz/unternehmensservice/innovation-und-technologieberatung/normung-und-normen/definition-normen-standards-3325396 (Zugriff am: 19. Juni 2023).

[30] RWB Rechtswörterbuch. „Verfassungsrecht: Richtlinie." https://www.rechtswoerterbuch.de/recht/r/richtlinien/ (Zugriff am: 19. Juni 2023).

[31] Prof. Dr.-Ing. Karl-Heinz Niemann, *IT-Sicherheit in Produktionsanlagen: Vorlesungsskript zur Vorlesung.* Zugriff am: 18. Juni 2023.

[32] BWLWissen.net. „Stakeholder." https://bwl-wissen.net/definition/stakeholder (Zugriff am: 19. Juni 2023).

[33] Baunetz_Wissen. „Glossar: VdS." https://www.baunetzwissen.de/glossar/v/vds-50339 (Zugriff am: 15. April 2023).

[34] Dipl.-Ing. (FH) Stefan Luber / Peter Schmitz. „Was ist Zero Trust Network Access (ZTNA)?: Definition Zero Trust Network Access (ZTNA)." https://www.security-insider.de/was-ist-zero-trust-network-access-ztna-a-959927/ (Zugriff am: 26. Juni 2023).

[35] IBM. „SD-WAN erklärt - Was ist Software-Defined WAN (SD-WAN)?" https://www.ibm.com/de-de/services/network/sd-wan